REDACTED

AO 108 (Rev. 06/09) Application for a Warrant by Telephone or Other Reliable Electronic Means to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Seizure of *(Briefly describe the property to be seized)* $266,720.00 IN U.S. CURRENCY HELD IN PNC BANK ACCOUNT NUMBER 5696913328	)	Case No. 22-202M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the _____ District of Delaware is subject to forfeiture to the United States of America under 18 U.S.C §§ 981 and 982, 21 USC §853(e)&(f), 28 USC §2461 *(describe the property)*:

See Attachment A

The application is based on these facts:

see attached AFFIDAVIT

☑ Continued on the attached sheet.

Applicant's signature

Nicholas Fuller, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 06/10/2022

Judge's signature

City and state: Wilmington, Delaware

Honorable Sherry R. Fallon, US Magistrate Judge

Printed name and title

ATTACHMENT A

All funds held by PNC Bank up to $266,720.00 held in PNC Bank account number 5696913328.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEIZURE OF $266,720.00 IN U.S. CURRENCY HELD IN PNC BANK ACCOUNT NUMBER 5696913328	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEIZE

I, Nicholas Fuller, ("Your Affiant" or "SA Fuller"), a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), Baltimore Division, Wilmington, Delaware, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant has been a SA with the FBI since July 5, 2020. As part of my duties, I investigate violations of federal law, including cyber-crime cases such as computer intrusions, cyber stalking, identity theft, internet fraud, and money laundering. I have gained expertise in conducting such investigations through training in seminars, classes, and everyday work related to the technical aspects of computer crimes.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41 to seize the property listed in Attachment A (the "SUBJECT PROPERTY"), currently being maintained by PNC Bank account number 5696913328 (the "SUBJECT BANK ACCOUNT"). The SUBJECT PROPERTY is more particularly described in Attachment A, which is incorporated into this Affidavit by reference.

4. Unless otherwise stated, the facts contained within this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. Because this affidavit is only submitted in furtherance of establishing probable cause, it does not set forth every fact I know about the matter. I have set forth only the facts that I believe are necessary to establish probable cause to seize the SUBJECT PROPERTY.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that individuals involved in a money-laundering Criminal Organization violated Title 18, United States Code, Sections 1343 (wire fraud) and 1956 (money laundering) (collectively, the "SUBJECT OFFENSES"), and that the funds held in the bank account listed in Attachment A are therefore subject to seizure and forfeiture to the United States as the proceeds of or property involved in the SUBJECT OFFENSES.

6. Moreover, based upon my experience, as well as discussions with other knowledgeable law enforcement officers, there is probable cause to believe that the SUBJECT PROPERTY is subject to forfeiture pursuant to Title 18, United States Code, Section 98l(a)(l)(C) and Title 28, United States Code, Section 2461, which provide for criminal and civil forfeiture of property that "constitutes or is derived from proceeds traceable to a violation of . . . any offense constituting 'specified unlawful activity,'" as defined in Title 18, United States Code, Section 1956 (c)(7), which includes wire fraud. In addition, there is probable cause to believe that the SUBJECT PROPERTY is subject to forfeiture pursuant to Title 18, United States Code, Section 982(a)(l), which provides for civil and criminal forfeiture of property involved in violations of Title 18, United States Code, Sections 1956 and 1957. Finally, the SUBJECT PROPERTY is subject to

seizure pursuant to Title 18, United States Code, Section 981(b) and Title 21, United States Code, Section 853(e) & (f) by Title 18, United States Code, Section 982(b)(l).

BACKGROUND TERMS

7. A Money Mule is an individual who receives the proceeds of criminal activity, often fraud, into his or her bank account and transfers those funds to other bank accounts at the direction of a criminal actor. Many Money Mules are victims of Romance Fraud schemes and may be unaware of the full extent of the criminal actions of the individuals conducting the underlying schemes. The use of Money Mules by a money-laundering criminal organization is part of the effort to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of their fraud schemes.

8. An automated clearing house (an "ACH") is a computer-based electronic network for processing transactions, usually domestic low value payments, between participating financial institutions. It may support both credit transfers and direct debits.

9. A Criminal Organization is an affiliated group of individuals working together to engage in criminal activity, most often fraud, and to launder the proceeds of that criminal activity. Criminal Organizations often engage in multiple kinds of criminal activities, operate on a transnational basis, have a hierarchy or comparable structure, and employ extensive supporting networks of Money Mules, both in the United States and abroad.

PROBABLE CAUSE

10. As explained in more detail below, there is probable cause to believe that a money-laundering Criminal Organization perpetrated a scheme to defraud the U.S. Small Business Administration ("SBA") by submitting fraudulent loan applications for COVID-19 relief funds and laundering the proceeds of the scheme through bank accounts opened by Money Mules and

other members of the Criminal Organization. There is also probable cause to believe that the SUBJECT PROPERTY represents proceeds of the Criminal Organization's conspiracy to defraud the SBA.

I. Background of the Investigation: January and March 2021 Search Warrants

11. In March 2020,[1] the SBA issued disaster declarations related to the novel 2019 coronavirus ("COVID-19") that emerged as a major public health crisis. As a result, the SBA received additional funding as part of its Economic Injury Disaster Loans ("EIDL") program to assist small businesses coping with the financial repercussions of COVID-19.

12. In or about August 2020, the owners of FARM A, a small farm located in Lincoln, Delaware, sought to obtain an EIDL loan. The owners of FARM A learned, however, that an unknown individual had already submitted a EIDL application to the SBA in or about June 21 on behalf of FARM A. Although the FARM A EIDL application used some of the owner's information, the owners had not submitted the application, nor were they aware that an application had been submitted on behalf of FARM A.

13. The fraudulent FARM A EIDL application had been submitted to the SBA from IP address 89.45.4.250. Subsequent investigation by the FBI and the Delaware State Police ("DSP") uncovered a Criminal Organization that had submitted ninety-five (95) additional EIDL applications to the SBA between June 20 and August 5 from the same IP address and using variations of the same five email addresses. Most of these EIDL applications listed farming or agriculture-related businesses as the applicants.

[1] Unless specified otherwise, all references to dates in this Affidavit occurred in 2020.

14. On the basis of this information, the FBI obtained a search warrant for five email addresses on January 28, 2021 (the "January search warrant") and a search warrant for two email addresses on March 11, 2021. The affidavit submitted in support of the January search warrant sets out more fully the background of the investigation and is attached to this Affidavit as Exhibit A. As explained in more detail in Exhibit A, which is incorporated into this Affidavit by reference, the investigation uncovered eighteen (18) fraudulent EIDL loans funded by the SBA totaling approximately $1.3 million that were submitted as part of the conspiracy to defraud the SBA. The FBI was able to interview almost all businesses that had been listed on the eighteen EIDL applications. None of those businesses had submitted EIDL applications.

II. Fraudulent EIDL for FARM B

15. One of the 18 fraudulent EIDL loans funded by the SBA was submitted on behalf of FARM B, a small farm located in Brighton, Colorado. On or about June 29, the funds related to the fraudulent FARM B EIDL, specifically $144,800, along with a $10,000 advance, were deposited by ACH transfer into a JP Morgan Chase Bank account ending in -2909 (the "Chase bank account"). The Chase bank account had been opened on June 22, a week before the FARM B EIDL deposit, by [redacted] doing business as ("dba") [redacted] [redacted] was the only authorized user and sole signatory on the Chase bank account.

16. In reality, the owners of the FARM B EIDL had not submitted the application for the EIDL. Further investigation revealed that [redacted] had opened the Chase bank account at the direction of a member of the Criminal Organization in order to launder the proceeds of the fraudulent EIDL scheme. For example, the day after the fraudulent FARM B EIDL was deposited into the Chase bank account, [redacted], again acting at the direction of a member of the Criminal Organization, wrote a $138,500 check to another member of the Criminal Organization. That

check was deposited into a separate bank account also opened to launder the proceeds of the fraudulent EIDL scheme. Based on these suspicious financial transactions, there is probable cause to believe that [redacted] served as a Money Mule for the Criminal Organization.

17. Further investigation revealed that the FARM B EIDL was not the only fraudulent EIDL deposited into a bank account opened and controlled by [redacted]. On July 8, 2020, the SBA deposited $149,900 into the same Chase bank account. Similarly, [redacted] opened a Citizen's Bank business checking account ending in -7099 (the "Citizens bank account") on July 1, 2020. Within two weeks, the Citizens bank account had received three deposits of $149,900—one on July 7 and two on July 13—each of which represented the proceeds of a fraudulent EIDL.

18. Upon receiving the EIDL funds into these accounts, [redacted], acting at the direction of the same member of the Criminal Organization, depleted the majority of the EIDL funds by sending checks from [redacted] accounts to other members within the Criminal Organization.

III. [redacted] PNC Bank Account and the SUBJECT PROPERTY

19. On June 6, 2020, [redacted] dba [redacted] LLC opened PNC bank account number 5696913328, the SUBJECT BANK ACCOUNT. The following month, consistent with the EIDL transactions described in paragraphs 14-18, the SUBJECT BANK ACCOUNT received $414,700 from 3 fraudulent EIDLs submitted to the SBA. Specifically, on July 7, the SUBJECT BANK ACCOUNT received a $149,900 ACH transfer from the SBA related to an EIDL submitted on behalf of a plumbing company based in Decatur, Alabama. On July 13, the SUBJECT BANK ACCOUNT received a $149,900 ACH transfer from the SBA related to an EIDL submitted on behalf of a metal mining company based in Brookwood, Alabama. The same day, July 13, the SUBJECT BANK ACCOUNT received a $114,900 ACH transfer from the SBA related to an EIDL submitted on behalf of a small farm in Wise, Virginia.

20. After the first EIDL was deposited into the SUBJECT BANK ACCOUNT on July 7, on or about the next day, [redacted] wrote a check for $147,980 to David S. Kaufman P.A for "services" written on the memo line. [redacted] wrote the check at the direction of the same member of the Criminal Organization. The Kaufman check was subsequently deposited into a separate bank account.

21. According to communications with PNC Bank, due to the multiple EIDLs submitted into the SUBJECT BANK ACCOUNT in the names of seemingly unrelated business, PNC Bank placed a hold on the SUBJECT BANK ACCOUNT, including the balance of $266,720.00 that remained in the account. PNC Bank statements for the SUBJECT BANK ACCOUNT demonstrate that, apart from the EIDL deposits, the only activity in the account involved a $200 initial deposit and $151.98 in small withdrawals and debit purchases. Accordingly, $266,720.00 represents the remainder of the three fraudulent SBA EIDLs, i.e., the SUBJECT PROPERTY, that were deposited into the SUBJECT BANK ACCOUNT.

22. Further investigation revealed that [redacted] opened the various bank accounts, including the SUBJECT BANK ACCOUNT, at the direction of a member of the Criminal Organization, who provided [redacted] with the name of [redacted] and business paperwork documenting the formation of [redacted] The same member of the Criminal Organization also provided [redacted] with instructions regarding where to transfer the proceeds of the EIDLs deposited into [redacted] various accounts. In exchange, [redacted] kept a portion of the proceeds for himself.

23. In summary, there is probable cause to believe that actors working for a Criminal Organization, some of whom have been identified, used the SUBJECT BANK ACCOUNT to receive funds from fraudulent EIDL applications submitted to the SBA. There is probable cause

that the SUBJECT BANK ACCOUNT was then used to launder a large portion of the funds to other members within the Criminal Organization. Finally, there is probable cause to believe that a portion of the stolen funds from the scheme to defraud the SBA, the SUBJECT PROPERTY, remains in the SUBJECT BANK ACCOUNT. As such, the SUBJECT PROPERTY constitutes proceeds traceable to violations of the SUBJECT FEDERAL OFFENSES and therefore may be seized for forfeiture.

CONCLUSION

24. Based on the information set forth in this affidavit, there is probable cause to believe that the SUBJECT PROPERTY constitutes proceeds traceable to violations of the above-listed federal offenses and therefore may be seized for forfeiture. Therefore, pursuant to Federal Rule of Criminal Procedure 41, I ask that this Court issue a warrant to seize the SUBJECT PROPERTY, more fully described in Attachment A, as fruits of violations of the federal offenses.

Respectfully submitted,

SA Nicholas Fuller, FBI

Sworn and subscribed before me
this 10th day of June 2022

Honorable Sherry R. Fallon
United States Magistrate Judge

Sworn to me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1

EXHIBIT A

SEALED

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with mikejohnn75@gmail.com, et al., that is stored at premises controlled by Google LLC

Case No. 21- 20M

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

see Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

see Attachment B

YOU ARE COMMANDED to execute this warrant on or before February 11, 2021 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to duty magistrate judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 4:30 p.m. 1/28/2021

Judge's signature

City and state: Wilmington, Delaware

Honorable Jennifer L. Hall, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: 21-	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

Special Agent Nicholas Fuller, FBI
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following email addresses, from the date of the creation of the respective accounts to the present, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Pkwy, Mountain View, CA 94043:

mikejohnn75@gmail.com

farm75550@gmail.com

adjenkins755@gmail.com

jamesmalcolm777@gmail.com

farm34001387@gmail.com

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from account creation to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The

Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code ("U.S.C.") § 371 (Conspiracy); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); and 18 U.S.C. § 1957 (Engaging in Monetary Transactions in Property Derived from a Specified Unlawful Activity); by an individual or individuals as yet unknown and occurring on or after the date of account creation to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of any fraud schemes, including preparatory steps taken in furtherance thereof; communications related to any fraudulent schemes, including communications to victims or between co-conspirators; and evidence of tools used to commit those crimes;

b. Evidence of any money laundering, including preparatory steps taken in furtherance thereof; communications related to any money laundering schemes, including communications to victims or between co-conspirators; and evidence of tools used to commit those crimes;

c. Evidence of familiarity with and use of social media;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to the identity of person(s) who communicated with the user ID about matters relating to fraud schemes and money laundering, including records that help reveal their whereabouts;

h. Records related to any additional victims of similar fraud schemes.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

SEALED

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with mikejohnn75@gmail.com, et al., that is stored at premises controlled by Google LLC

Case No. 21- 20M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

see Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

☐ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime; ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 371	Conspiracy
18 USC 1341	Mail Fraud
18 USC 1343	Wire Fraud
18 USC 1956	Laundering of Monetary Instruments
18 USC 1957	Engaging in Monetary Transactions in Property Derived from a Specified Unlawful Activity

The application is based on these facts:

see attached Affidavit

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nicholas Fuller, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: January 28, 2021

Judge's signature

City and state: Wilmington, Delaware

Jennifer L. Hall, United States Magistrate Juge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH mikejohnn75@gmail.com, et al., THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	:	Case No. 21- 20M **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Fuller, ("Your Affiant" or "SA Fuller"), a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), Baltimore Division, Wilmington, Delaware, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant has been a SA with the FBI since July 5, 2020. As part of my duties, I investigate violations of federal law, including cyber-crime cases such as computer intrusions, cyber stalking, identity theft, and internet fraud. I have gained expertise in conducting such investigations through training in seminars, classes, and everyday work related to the technical aspects of computer crimes. Prior to joining the FBI, I was employed at Citibank as an analyst in the financial regulatory department for six years. In particular, I gained expertise reviewing Dodd Frank regulations enacted in response to the 2008 financial crisis. Before that I worked at Bank of America as an Operations Specialist dealing with mortgage bankruptcies. I am working this investigation with SA Jeffrey A. Reising, who took the lead on this investigation and has extensive experience working cyber-crime cases involving international money-laundering enterprises.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a search warrant for information associated with certain email accounts stored at the premises controlled by Google LLC. (hereinafter, "GOOGLE"), an email provider headquartered at 1600 Amphitheatre Pkwy, Mountain View, CA 94043. The email accounts to be searched are more particularly described as Gmail accounts bearing the screen name or email address set forth below and in Attachment A. Specifically, the email addresses to be searched are as follows:

mikejohnn75@gmail.com ("TARGET ACCOUNT 1"),

farm75550@gmail.com ("TARGET ACCOUNT 2"),

adjenkins755@gmail.com ("TARGET ACCOUNT 3"),

jamesmalcolm777@gmail.com ("TARGET ACCOUNT 4"),

farm34001387@gmail.com ("TARGET ACCOUNT 5"),

Collectively, the email accounts will be referred to as the "TARGET ACCOUNTS."

4. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and is related to a scheme to defraud the United States Small Business Administration ("SBA"). As explained in more detail below, the search warrant would require GOOGLE to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. Based on my training and experience, and the facts as set forth in this affidavit, Your Affiant believes there is probable cause that the TARGET ACCOUNTS contain evidence of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 1341 (Mail Fraud); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); and 18 U.S.C. § 1957

(Engaging in Monetary Transactions in Property Derived from a Specified Unlawful Activity) (collectively, the "TARGET FEDERAL OFFENSES") that have been committed by an individual or individuals as yet unknown. The information to be searched is described in the following paragraphs and in Attachment A.

6. Unless otherwise stated, all information contained in this affidavit is either personally known to Your Affiant through his own investigation – through conducting interviews, reviewing subpoena materials and other records, etc. – or has been related to Your Affiant by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of violations of the TARGET FEDERAL OFFENSES are presently located in the TARGET ACCOUNTS.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

TECHNICAL BACKGROUND AND TERMS

8. In my training and experience, I have learned that GOOGLE provides a variety of on-line services, including electronic mail ("email") access, to the public. GOOGLE allows subscribers to obtain email accounts at various domain names, such as www.gmail.com, including the accounts listed in Attachment A. Subscribers obtain an account by registering with GOOGLE. During the registration process, GOOGLE asks subscribers for basic personal information. Thus,

the computers of GOOGLE are likely to contain stored electronic communications (including retrieved and unretrieved email for GOOGLE subscribers) and information concerning subscribers and their use of GOOGLE services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the TARGET FEDERAL OFFENSES because the information can be used to identify the account's user or users.

9. GOOGLE subscribers can also store files with GOOGLE in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by GOOGLE. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

10. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account numbers). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

11. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e.,

session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, such information can help identify computers or other devices used to access the email account.

12. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained

by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

14. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. An "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing, Internet Protocol version 4 ("IPv4"), consists of four numbers between 0 and 255 separated by dots, e.g. 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet

Service Providers ("ISP") assign IP addresses to their customers' computers. ISPs typically log their customers' connections, which mean that the ISP can identify which of their customers are assigned a specific IP address during a particular session. Most Internet traffic is routed via IPv4, but Internet Protocol version 6 ("IPv6") is also being used.

16. IPv6 is the most recent version of the IP, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. Every device on the Internet is assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization, more addresses were required than IPv4 had available. IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334, but methods to abbreviate this full notation exist.

17. A "server" is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located anywhere. For example, it is not uncommon for a network server to be located hundreds, or even thousands, of miles away from the client's computer.

18. Telephone calls and text messages sent over the Internet contain IP addresses that can be used to determine the origin and destination of the messages. These IP addresses may be traced to determine the sender of a specific telephone call or text message.

19. "Geolocation" is, in general, the process of identifying an IP address's geographical location, including its country of origin, which in turn helps identify the location of the device connected to the Internet using that IP address.

20. A Virtual Private Server ("VPS") is a server created using software virtualization. It functions like a physical server, but it is a virtualized instance created within a server.

PROBABLE CAUSE TO SEARCH THE TARGET ACCOUNTS

21. As explained in more detail below, Your Affiant believes that probable cause exists to show that the TARGET ACCOUNTS are being used by members of a Criminal Organization (the "Criminal Organization"), to perpetrate and facilitate a fraud against the SBA, an agency of the United States government. In support of this application, Your Affiant asserts the following:

I. Background of the Investigation

22. As relevant to this Affidavit, the SBA administers the Economic Injury Disaster Loans ("EIDL") program, which is designed to provide long-term, low-interest loans to small businesses that have experienced substantial economic injury as a result of a declared disaster. In March 2020, a novel strain of coronavirus ("COVID-19") emerged as a public health crisis and led to a global pandemic. In response to the COVID-19 pandemic, many states in the U.S. implemented lockdowns that affected the ability of small businesses to maintain operations. The SBA also issued disaster declarations for all U.S. states and territories in March 2020. Accordingly, small businesses that experienced temporary loss of revenue due to the COVID-19 pandemic became eligible for an SBA EIDL. The maximum amount of such EIDL loans is currently $150,000. EIDL loans appear in the recipient's identified bank account as a deposit from the U.S. Treasury in the amount of the loan, minus a $100 fee.

23. The EIDL application requires an applicant to supply an email address that serves as the primary means of communication between the applicant and the SBA. In order to expedite processing and provide relief as soon as possible, most communication from the SBA regarding the EIDL is sent via email to the email address provided on the EIDL application.

24. [redacted] own [redacted] in Lincoln, Delaware, within the District of Delaware. Because of the COVID-19 pandemic, the [redacted] sought to obtain an EIDL loan from the SBA for their farming business. [redacted] researched the SBA EIDL program and initiated an application in or about August of 2020.

25. According to [redacted] soon after she started the application, she received a package via U.S. Mail from the SBA regarding an EIDL loan on behalf of [redacted] According to a "Loan Authorization and Agreement," the SBA had approved an EIDL loan for [redacted] on June 22, 2020 in the amount of $145,600. The paperwork indicated that the [redacted] would be required to begin repayment in June 2021 by making $710 monthly installment payments for thirty (30) years:

SBA Loan #1362128004 Application #3305682872

U.S. Small Business Administration

Economic Injury Disaster Loan

LOAN AUTHORIZATION AND AGREEMENT

Date: 06.22.2020 (Effective Date)

On the above date, this Administration (SBA) authorized (under Section 7(b) of the Small Business Act, as amended) a Loan (SBA Loan #1362128004) to [redacted] f [redacted] Lincoln Delaware 19960 in the amount of one hundred and forty-five thousand six hundred and 00/100 Dollars ($145,600.00), upon the following conditions:

PAYMENT

- Installment payments, including principal and interest, of $710.00 Monthly, will begin Twelve (12) months from the date of the promissory Note. The balance of principal and interest will be payable Thirty (30) years from the date of the promissory Note.

INTEREST

- Interest will accrue at the rate of 3.75% per annum and will accrue only on funds actually advanced from the date(s) of each advance.

26. In reality, the [redacted] had not completed and submitted an EIDL application to the SBA. Ms. [redacted] thereafter contacted the SBA and was advised that an individual claiming to be [redacted] had contacted the SBA in August 2020 using a telephone number that was unfamiliar

to the [redacted] Ms. [redacted] also advised that while her husband's first name is [redacted] he goes by his middle name, [redacted] As explained in more detail below, although the fraudulent [redacted] EIDL application listed some accurate information about [redacted] the application listed TARGET ACCOUNT 1 as the contact email address.

27. The SBA informed [redacted] that the agency had funded the fraudulent [redacted] Farm EIDL to a Woodforest National Bank ("Woodforest") account ending in -1481 (the "Woodforest -1481 Account"). SBA records also reflect that although the funding account provided to the SBA in connection with the [redacted] loan changed, the Woodforest -1481 Account was initially provided to the SBA as the account into which the [redacted] EIDL funds were intended to be deposited.[1] SBA records listed Gattis Farm as the account holder on the Woodforest -1481 Account:

10/19/2020 WaterGirl Farm - 6840654 - Bank Accounts - U.S. Small Business Administration CALC Application

Hello, Fernanda Filotel (/Account/Manage) (SBA Team Lead)! | 0 Request help () | Log off (/Account/LogOff)

Admin panel (/Administration) Existing Deals (/) Tasks (https://rapidsba2.sba.gov)

Home (/) / Application (/LeadTileaId=6840654) / Rapid Decision (/CalculatorHeadId=6840654) / Bank Account

Bank Account

Account Type	Account Number	Routing Number	Name Of Bank	Name On Account	Account Status	Account Ownership Status
Checking	1111001481	053112592	WOODFOREST NATIONAL BANK	Gattis Farm	Cannot Verify	Cannot Authenticate

[1] Although the exact funding sequence attempted by the SBA is somewhat unclear, the available documents indicate that the SBA attempted to fund the [redacted] EIDL multiple times using multiple bank accounts. Your Affiant has requested additional documentation from the SBA for clarification.

28. When [redacted] contacted Woodforest, she was advised that although the SBA had attempted to transfer the funds to the Woodforest -1481 Account, the money had been refused and returned.

29. On September 16, 2020, [redacted] contacted the Delaware State Police ("DSP"), which opened an investigation. The fraudulent [redacted] EIDL has affected the [redacted] credit and interfered with their ability to receive a legitimate EIDL from the SBA.

II. Law Enforcement Uncovers Scheme Involving Additional Fraudulent EIDLs

30. On October 30, 2020, SA Reising contacted DSP Detective Sergeant Morris, who had been investigating the [redacted] fraud. The FBI assumed the lead investigative role in a joint case with the DSP and the SBA Office of the Inspector General ("SBA-OIG").

A. 96 EIDL Applications Submitted from IP Address 89.45.4.250

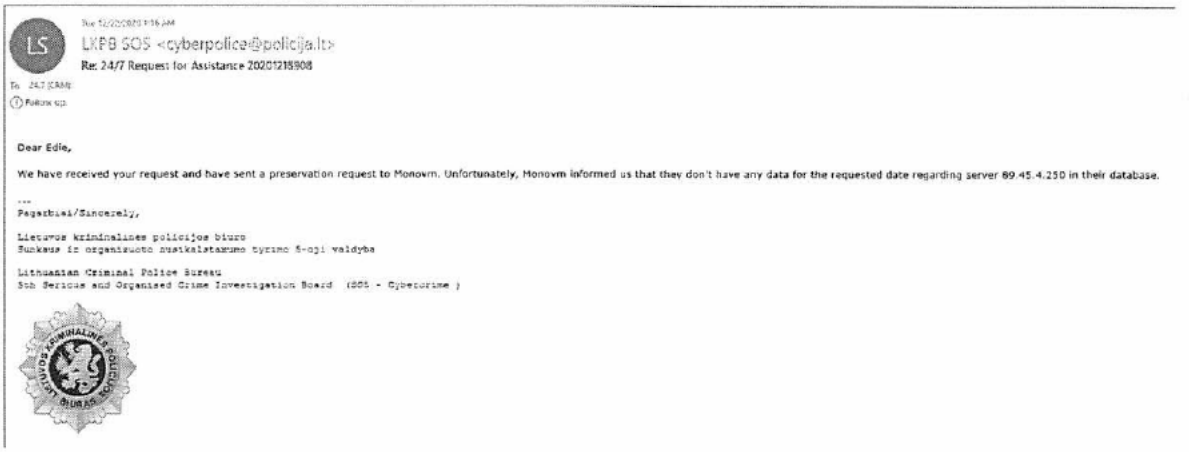
31. Further investigation revealed that on June 21, 2020 at 9:05 am, an unknown member of the Criminal Organization accessed the SBA servers and submitted the fraudulent [redacted] Farm EIDL application in the name of [redacted] doing business as ("d/b/a") [redacted] Farm. According to SBA records, the individual accessed SBA's system from IP address 89.45.4.250.

32. IP address 89.45.4.250 is owned by M247 Limited ("M247"), a Los Angeles, California, company that provides internet infrastructure services, including web hosting:

33. On December 9, 2020, M247 advised that IP address 89.45.4.250 was assigned to MonoVM Networks ("MonoVM"), a Lithuanian company specializing in VPSs:

Screen captures from https://monovm.com/ by SA Reising on January 5, 2021.

34. The U.S. Department of Justice requested records from MonoVM related to IP address 89.45.4.250 for the time period associated with the [redacted] EIDL application. According to Lithuanian law enforcement, MonoVM did not have data available:



LKPB SOS <cyberpolice@policija.lt>
Re: 24/7 Request for Assistance 20201218908

Dear Edie,

We have received your request and have sent a preservation request to Monovm. Unfortunately, Monovm informed us that they don't have any data for the requested date regarding server 89.45.4.250 in their database.

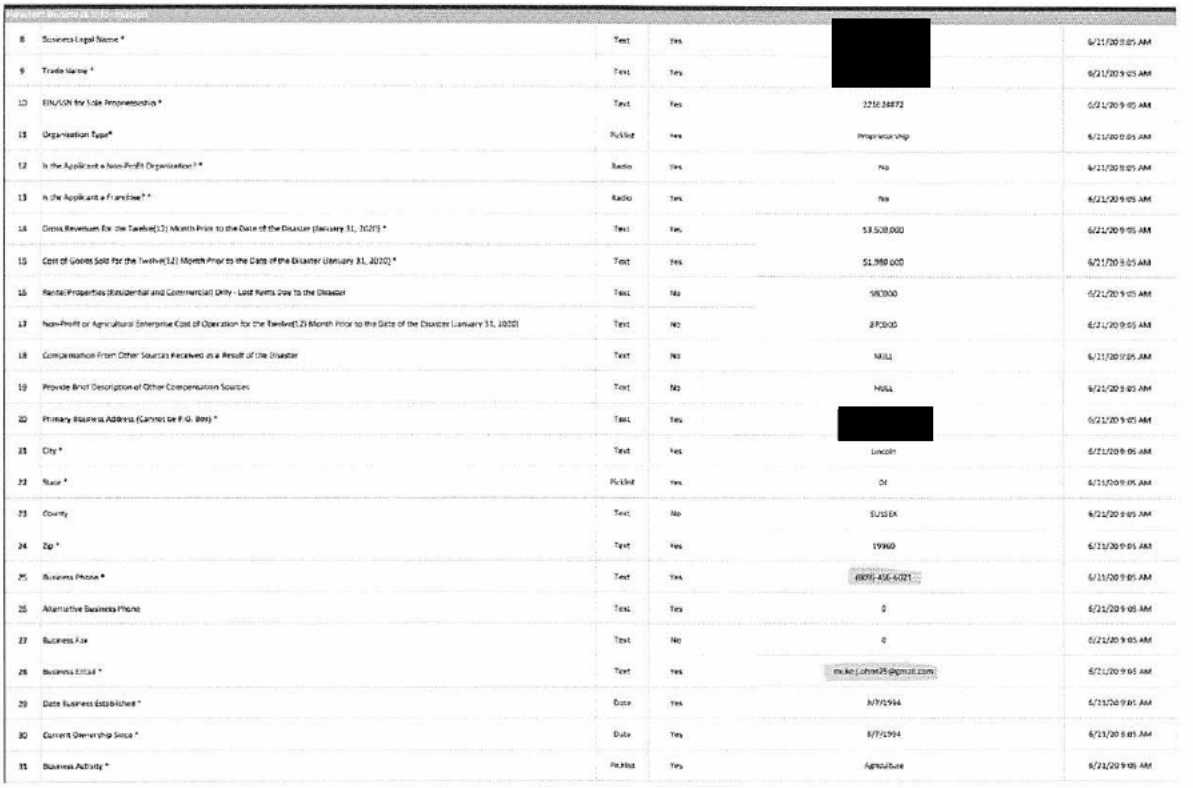
Pagarbiai/Sincerely,

Lietuvos kriminalinės policijos biuro
Sunkaus ir organizuoto nusikalstamumo tyrimo 6-oji valdyba

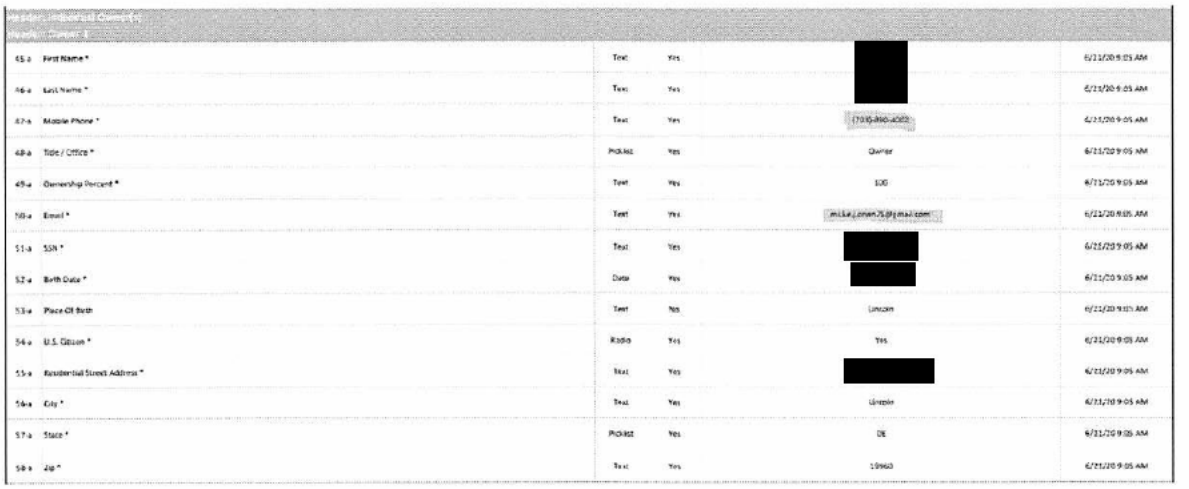
Lithuanian Criminal Police Bureau
6th Serious and Organised Crime Investigation Board (6OS - Cybercrime)

35. Your Affiant knows based on conversations with senior FBI agents that transnational criminal organizations often utilize VPS providers such as MonoVM in order to obtain a US-based IP address and thereby make it appear that an individual is operating in the United States. Your Affiant is also aware that transnational criminal organizations often utilize foreign VPS services specifically because records related to the identity of a subscriber are difficult to obtain and frequently unavailable once the VPS contract is completed.

36. As noted above, the [redacted] application listed certain fragments of [redacted] personal information that were accurate—Name, Date of Birth, Social Security Number, Address—but provided incorrect telephone numbers and TARGET ACCOUNT 1 as the contact email address:



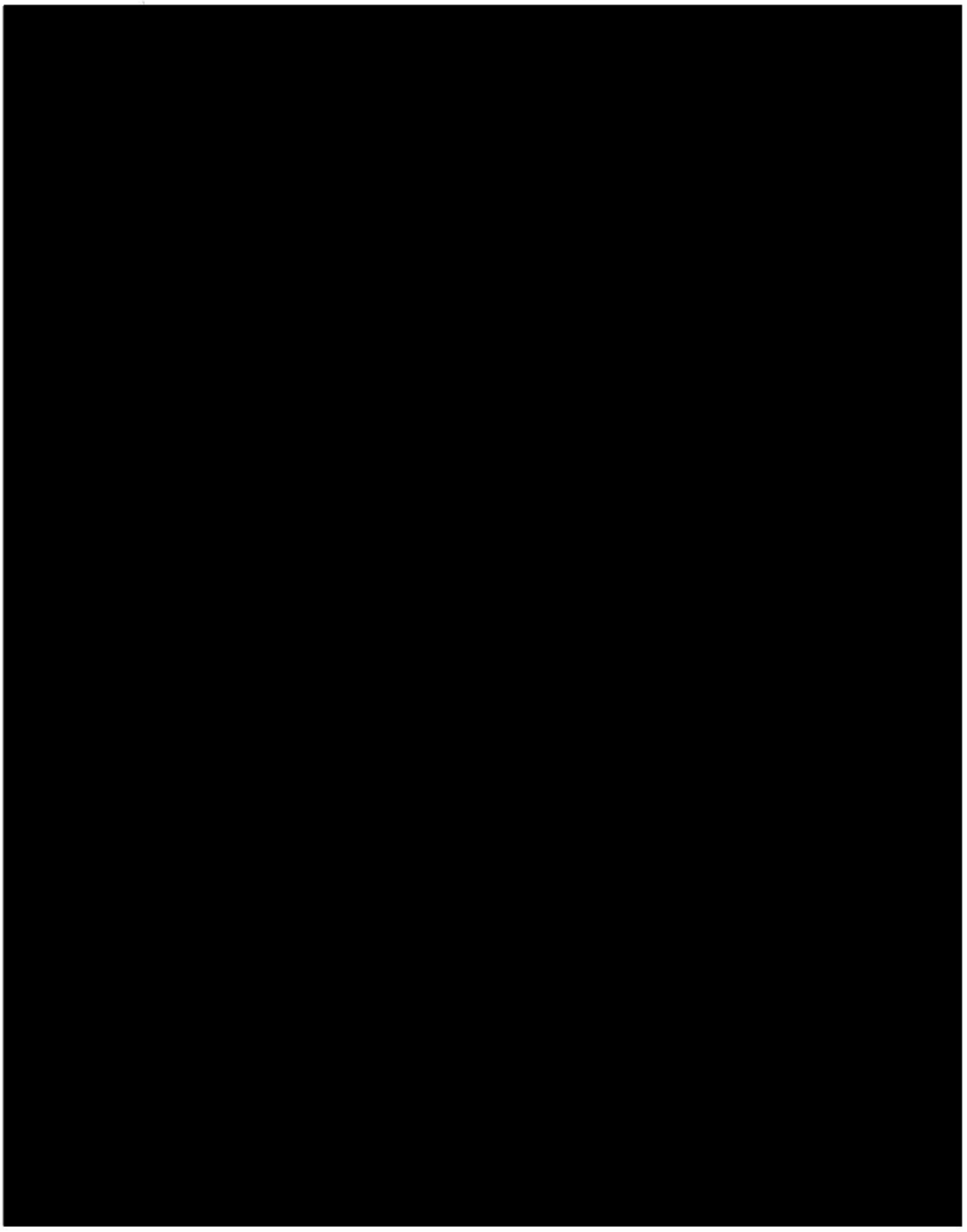
8	Business Legal Name *	Text	Yes	[redacted]	6/21/20 9:05 AM
9	Trade Name *	Text	Yes		6/21/20 9:05 AM
10	EIN/SSN for Sole Proprietorship *	Text	Yes	225534872	6/21/20 9:05 AM
11	Organization Type*	Picklist	Yes	Proprietorship	6/21/20 9:05 AM
12	Is the Applicant a Non-Profit Organization? *	Radio	Yes	No	6/21/20 9:05 AM
13	Is the Applicant a Franchise? *	Radio	Yes	No	6/21/20 9:05 AM
14	Gross Revenues For the Twelve(12) Month Prior to the Date of the Disaster (January 31, 2020) *	Text	Yes	$3,500,000	6/21/20 9:05 AM
15	Cost of Goods Sold For the Twelve(12) Month Prior to the Date of the Disaster (January 31, 2020) *	Text	Yes	$1,980,000	6/21/20 9:05 AM
16	Rental Properties (Residential and Commercial) Only - Last Rents Due to the Disaster	Text	No	$80000	6/21/20 9:05 AM
17	Non-Profit or Agricultural Enterprise Cost of Operation for the Twelve(12) Month Prior to the Date of the Disaster (January 31, 2020)	Text	No	$70000	6/21/20 9:05 AM
18	Compensation From Other Sources Received as a Result of the Disaster	Text	No	NULL	6/21/20 9:05 AM
19	Provide Brief Description of Other Compensation Sources	Text	No	NULL	6/21/20 9:05 AM
20	Primary Business Address (Cannot be P.O. Box) *	Text	Yes	[redacted]	6/21/20 9:05 AM
21	City *	Text	Yes	Lincoln	6/21/20 9:05 AM
22	State *	Picklist	Yes	DE	6/21/20 9:05 AM
23	County	Text	No	SUSSEX	6/21/20 9:05 AM
24	Zip *	Text	Yes	19960	6/21/20 9:05 AM
25	Business Phone *	Text	Yes	(302) 436-6021	6/21/20 9:05 AM
26	Alternative Business Phone	Text	Yes	0	6/21/20 9:05 AM
27	Business Fax	Text	No	0	6/21/20 9:05 AM
28	Business Email *	Text	Yes	mike.lohner75@gmail.com	6/21/20 9:05 AM
29	Date Business Established *	Date	Yes	8/7/1994	6/21/20 9:05 AM
30	Current Ownership Since *	Date	Yes	8/7/1994	6/21/20 9:05 AM
31	Business Activity *	Picklist	Yes	Agriculture	6/21/20 9:05 AM



45-a	First Name *	Text	Yes	[redacted]	6/21/20 9:05 AM
46-a	Last Name *	Text	Yes		6/21/20 9:05 AM
47-a	Mobile Phone *	Text	Yes	(703) 946-4082	6/21/20 9:05 AM
48-a	Title / Office *	Picklist	Yes	Owner	6/21/20 9:05 AM
49-a	Ownership Percent *	Text	Yes	100	6/21/20 9:05 AM
50-a	Email *	Text	Yes	mike.lohner75@gmail.com	6/21/20 9:05 AM
51-a	SSN *	Text	Yes	[redacted]	6/21/20 9:05 AM
52-a	Birth Date *	Date	Yes	[redacted]	6/21/20 9:05 AM
53-a	Place Of Birth	Text	Yes	Lincoln	6/21/20 9:05 AM
54-a	U.S. Citizen *	Radio	Yes	Yes	6/21/20 9:05 AM
55-a	Residential Street Address *	Text	Yes	[redacted]	6/21/20 9:05 AM
56-a	City *	Text	Yes	Lincoln	6/21/20 9:05 AM
57-a	State *	Picklist	Yes	DE	6/21/20 9:05 AM
58-a	Zip *	Text	Yes	19960	6/21/20 9:05 AM

37. Upon further review, SBA-OIG discovered 96 additional EIDL loan applications that had been submitted from the same IP address as the fraudulent [redacted] application. The applications purported to be affiliated with farms or agricultural businesses and came from states across the country:

Table 1: 96 EIDL Applications



B. The 96 EIDL Applications Used Same 5 Email Addresses

38. Each of the 96 EIDL applications used variations of the same five email accounts to submit the applications. As explained below, although each of the 96 EIDL applications had dots embedded within the email addresses provided, in reality, the applications were submitted using the TARGET ACCOUNTS.

39. According to Google, when a subscriber owns a particular email address, the subscriber owns all variations of that email address, including variations that contain dots:

Dots don't matter in Gmail addresses

If someone accidentally adds dots to your address when emailing you, you'll still get that email. For example, if your email is johnsmith@gmail.com, you own all dotted versions of your address:

- john.smith@gmail.com
- jo.hn.sm.ith@gmail.com
- j.o.h.n.s.m.i.t.h@gmail.com

Note: If you use Gmail through work, school, or other organization (like yourdomain.com or yourschool.edu), dots do change your address. To change the dots in your username, contact your admin.

Screen capture from https://support.google.com/mail/answer/7436150?hl=en from SA Reising on January 5, 2021.

40. As reflected in Table 1 above, the individual submitting the 96 EIDL applications to the SBA was therefore able to submit multiple applications using variations of the TARGET ACCOUNTS. In the SBA's system, however, the email accounts appeared to be associated with different email accounts.

41. Records provided by Google indicate that the TARGET ACCOUNTS were all created in June or July 2020 and repeatedly logged into from IP address 89.45.4.250, the same IP address used to submit the 96 EIDL applications.

42. Records provided by Google also indicated that the TARGET ACCOUNTS were interconnected through their use of recovery email addresses. A recovery email address is a separate email account that serves as a security feature for a primary email account in case a subscriber loses a password or username or is otherwise unable to access the primary account. Your Affiant is aware that individuals perpetrating crimes through the use of fraudulent email addresses create multiple email addresses and provide other email addresses they control as recovery email addresses.

43. Google provided records that indicated that farm75550@gmail.com and adjenkins755@gmail.com, TARGET ACCOUNTS 2 and 3, listed mikejohnn75@gmail.com TARGET ACCOUNT 1, as the recovery email address. In turn, TARGET ACCOUNT 1 listed TARGET ACCOUNT 3 as its recovery email address. Similarly, jamesmalcolm777@gmail.com and farm34001387@gmail.com, TARGET ACCOUNTS 4 and 5, listed each other as recovery email addresses.

C. SBA Funded Eighteen Fraudulent EIDLs

44. Of the 96 EIDL loan applications identified in connection with the above-referenced IP address and email accounts, data from SBA-OIG indicate that the eighteen EIDLs

set forth in the following table were designated as funded or in the process of being funded. The value of these loans totaled $3,144,400.00:

Table 2: Funded EIDLS

Application	ClientIP	Current Stag	Original Loan Amou	Loan Amoun	Loan Numbe
3312704676	89.45.4.250	Funded	$147,000.00	$147,000.00	4396588200
3310203025	89.45.4.250	Funding	$39,600.00	$39,600.00	2624928101
3310414236	89.45.4.250	Funded	$148,100.00	$148,100.00	1521588207
3310658691	89.45.4.250	Funded	$149,400.00	$149,400.00	2052658205
3309562721	89.45.4.250	Funding	$147,800.00	$147,800.00	1617838106
3305913527	89.45.4.250	Funded	$148,900.00	$148,900.00	7317038010
3307174877	89.45.4.250	Funded	$60,100.00	$60,100.00	4509008100
3308489710	89.45.4.250	Funded	$143,700.00	$143,700.00	5966358100
3310129157	89.45.4.250	Funding	$149,200.00	$149,200.00	2319108106
3310123633	89.45.4.250	Funded	$149,700.00	$149,700.00	2271298106
3305600826	89.45.4.250	Funded	$124,400.00	$124,400.00	5987658008
3305847832	89.45.4.250	Funded	$144,800.00	$144,800.00	3541258002
3305831964	89.45.4.250	Funded	$130,200.00	$130,200.00	3529398006
3305794596	89.45.4.250	Funded	$146,700.00	$146,700.00	3505538006
3305623213	89.45.4.250	Funded	$148,600.00	$148,600.00	7300568009
3305627356	89.45.4.250	Funding	$144,500.00	$144,500.00	3202808007
3305630502	89.45.4.250	Funded	$145,900.00	$145,900.00	3219238009
3305681333	89.45.4.250	Funded	$144,500.00	$144,500.00	3317918005
			$3,144,400.00		

45. The FBI has interviewed eight of the individuals and businesses listed Table 2. None of these individuals or businesses submitted the listed EIDL applications with the SBA.

46. Based on the foregoing, Your Affiant submits that probable cause exists to believe that each of the 96 EIDL applications were fraudulent and submitted as part of a conspiracy to defraud the SBA; that the TARGET ACCOUNTS were used in furtherance of that fraudulent scheme; and that the TARGET ACCOUNTS will contain evidence, fruits, and or instrumentalities of the TARGET FEDERAL OFFENSES.

III. Data Retention and Time Frame

47. Despite the passage of time, based upon my training and experience, I believe that evidence, fruits, and instrumentalities of the TARGET FEDERAL OFFENSES will be found in the custody and control of GOOGLE with regard to the TARGET ACCOUNTS for two primary reasons. First, pursuant to 18 U.S.C. § 2703(f), preservation requests were sent to GOOGLE

regarding each of the TARGET ACCOUNTS after each account was identified and updated as necessary. Second, generally speaking, an email that is sent to a GOOGLE subscriber is stored in the subscriber's "mail box" on GOOGLE's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on those servers indefinitely. Moreover, even if the subscriber deletes the email, it may continue to be available on GOOGLE servers for a certain period of time.

48. In Attachment B, Section II, Your Affiant requests permission to seize information from the TARGET ACCOUNTS going back to the date each of the TARGET ACCOUNTS was created. Your Affiant submits that there is probable cause to believe that evidence of the TARGET FEDERAL OFFENSES (including information related to the identity, user, or creator of the accounts) will be found in the TARGET ACCOUNTS going back to that date.

CONCLUSION

49. Based on the forgoing, Your Affiant respectfully requests that the Court issue the proposed search warrant. Because the warrant will be served on GOOGLE who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

50. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or

tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

SA Nicholas Fuller, FBI

Sworn and subscribed before me
this 28 day of January, 2021

Honorable Jennifer L. Hall
United States Magistrate Judge

Attested via telephone pursuant to F.R.Cr.P. 4.1

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following email addresses, from the date of the creation of the respective accounts to the present, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Pkwy, Mountain View, CA 94043:

mikejohnn75@gmail.com

farm75550@gmail.com

adjenkins755@gmail.com

jamesmalcolm777@gmail.com

farm34001387@gmail.com

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from account creation to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The

Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code ("U.S.C.") § 371 (Conspiracy); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1341 (Mail Fraud); 18 U.S.C. § 1956 (Laundering of Monetary Instruments); and 18 U.S.C. § 1957 (Engaging in Monetary Transactions in Property Derived from a Specified Unlawful Activity); by an individual or individuals as yet unknown and occurring on or after the date of account creation to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of any fraud schemes, including preparatory steps taken in furtherance thereof; communications related to any fraudulent schemes, including communications to victims or between co-conspirators; and evidence of tools used to commit those crimes;

b. Evidence of any money laundering, including preparatory steps taken in furtherance thereof; communications related to any money laundering schemes, including communications to victims or between co-conspirators; and evidence of tools used to commit those crimes;

c. Evidence of familiarity with and use of social media;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

e. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to the identity of person(s) who communicated with the user ID about matters relating to fraud schemes and money laundering, including records that help reveal their whereabouts;

h. Records related to any additional victims of similar fraud schemes.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 109 (Rev. 11/13) Warrant by Telephone or Other Reliable Electronic Means to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Seizure of *(Briefly describe the property to be seized)* $266,720.00 IN U.S. CURRENCY HELD IN PNC BANK ACCOUNT NUMBER 5696913328	)	Case No. 22-202M

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the _____ District of Delaware be seized as being subject to forfeiture to the United States of America. The property is described as follows:

see Attachment A

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 06/24/2022
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to Honorable Sherry R. Fallon .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 06/10/2022 12:43 pm

Judge's signature

City and state: Wilmington, Delaware

Honorable Sherry R. Fallon, US Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return

Case No.: 22-	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Print Save As... Reset

ATTACHMENT A

- $266,720.00 IN U.S. CURRENCY HELD IN PNC BANK ACCOUNT NUMBER 5696913328